

AB:ADG

UNITED STATES DISTRICT COURT  
EASTERN DISTRICT OF NEW YORK

IN THE MATTER OF THE SEARCH OF  
A BLACK LENOVO THINKPAD, MODEL  
E67 AND MACHINE TYPE 2522 WITH  
SERIAL NUMBER R8-B474X

**APPLICATION FOR A SEARCH  
WARRANT FOR AN ELECTRONIC  
DEVICE**

Case No. 19-M-216

**AFFIDAVIT IN SUPPORT OF AN  
APPLICATION UNDER RULE 41 FOR  
WARRANTS TO SEARCH AND SEIZE**

I, George Lane, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the DEVICE described in Attachment A for the things described in Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation ("FBI") and have been since March 2018. Previously, I worked as a Police Officer for the Philadelphia Police Department for approximately eight years. I am currently assigned to the Violent Crimes Task Force with the FBI. In that position, I have had significant training and experience investigating a wide range of crimes involving violence and threats of violence, including threats made by telephone, online and through other electronic means. I am familiar with the facts and circumstances set forth below from my participation in the investigation; my review of the investigative file, including the defendant's criminal history

record; and from reports of other law enforcement officers involved in the investigation.

Unless specifically indicated, all conversations and statements described in this affidavit are related in sum and substance and in part only.

3. The information provided below is provided for the limited purpose of establishing sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. Based on the facts set forth in this affidavit, there is probable cause to believe that the DEVICE described in Attachment A contains evidence, instrumentalities or fruits of criminal activity in violation of 18 U.S.C. §§ 2261(A)(1) and (2), concerning stalking, and 18 U.S.C. § 875(c), concerning threatening interstate communications.

#### **THE DEVICE**

4. The DEVICE is a black Lenovo ThinkPad, model number E67 and machine type 2522, with serial number R8-B474X.

#### **PROBABLE CAUSE**

5. Between approximately Fall of 2013 until Summer of 2016, the defendant FRANK SEGUI<sup>1</sup> was a graduate student at a University located within the Western District

---

<sup>1</sup> SEGUI was arraigned on a complaint before the Honorable Steven L. Tiscione on or about February 25, 2019. See 19-M-172 (SLT), Dkt. No. 3.

of Michigan (the "UNIVERSITY"). At the UNIVERSITY, the SEGUI was a research assistant for a professor ("JOHN DOE").

6. By at least October 2015, SEGUI became very angry with JOHN DOE and blamed DOE for his lack of success at the UNIVERSITY. In or about October 2015, SEGUI sent an email to DOE, copying numerous other individuals at the UNIVERSITY, listing his grievances with DOE and stating that DOE had broken numerous promises to him.

7. At some point after this email was sent, an individual at the UNIVERSITY told SEGUI that he could receive a Master's Degree but could no longer continue his other graduate studies at the UNIVERSITY.

8. In approximately June 2018, SEGUI moved back from Michigan to Brooklyn to live with his parents in Brooklyn, New York (the "Parents' Apartment"), where he resided until in or about February 2019.

9. On or about October 30, 2018, SEGUI sent an email to JOHN DOE, copying other members of the UNIVERSITY (the "October 2018 Email"). In this email, SEGUI wrote, in part, "It's now been 3 years and you people will still not leave me alone. [JOHN DOE] or one of you mother fuckers is telling every person I contact not to hire me. . . . I get it. This is a thing you universities do. . . . First you push them away then you do whatever you can to make them come back to you even if it means ruining their life even if they beg you leave them alone. You need to understand someone though. You're all monsters. You



don't deserve life. The world would be better without you. [JOHN DOE] I'm so glad that son of yours is a mute deformed autistic little shit. That's probably god's way of putting you in place. . . . What's fucked up is I know you guys covered your tracks anything short of tying you down and cutting off your fingers there no way you will ever admit to any wrong doing. You'll just claim I'm crazy and continue ruining my life till the day I die. . . ."

10. Based on the IP Address used to access the DEVICE, I learned that SEGUI sent the October 2018 Email from Brooklyn, New York.

11. JOHN DOE told law enforcement that, when he received the October 2018 Email, he felt threatened and fearful for his safety and the safety of his son, especially because SEGUI specifically mentioned DOE's son in the email. Based on his interactions with SEGUI, DOE felt that this was a credible threat from SEGUI.

12. On or about February 22, 2019, SEGUI traveled to the Port Authority Bus Terminal in Manhattan and had a ticket to take a bus from New York to Detroit, Michigan. While at the bus terminal, SEGUI was arrested for disorderly conduct by a Port Authority of New York and New Jersey Police Officer. SEGUI also resisted arrested.

13. Following his arrest, SEGUI was given Miranda warnings and agreed to speak with law enforcement. SEGUI then stated, in sum and substance and in part, that he was planning to travel to Michigan to kill JOHN DOE. SEGUI stated that he had previously purchased an axe on the Internet to kill DOE, but he did not have access to it because it was

in his parents' apartment in Brooklyn and, due to a fight with them several days earlier, he could not return. SEGUI also stated that, therefore, when he got to Michigan, he would go to a hardware store in the city where the UNIVERSITY is located to purchase another axe and that he would use that axe to kill DOE. SEGUI also stated which motel he would stay at before killing DOE.

14. SEGUI also stated in this interview that he had been monitoring JOHN DOE's publicly available teaching schedule so that he could follow DOE's locations throughout the day and be able to locate DOE in order to kill him.

15. Law enforcement agents spoke to the SEGUI's father at the Parents' Apartment. The father stated that he had recently kicked out SEGUI from the Parents' Apartment and that he was not welcome to return. SEGUI abandoned, among other items, the axe and DEVICE when he left the Parents' Apartment. Law enforcement subsequently received from the SEGUI's father consent to search SEGUI's former room and closet at the Parents' Apartment. During the course of the search, I observed the DEVICE. SEGUI's father said that the DEVICE belonged to SEGUI, SEGUI most likely sent the October 2018 Email from the DEVICE and that the parents did not use the DEVICE. Law enforcement agents also located the axe purchased on the Internet as described by SEGUI, as well as the sheath that contained the axe and the packaging for the axe addressed SEGUI

16. Among other evidence, a search of the DEVICE will likely reveal evidence of SEGUI's online order for the axe, other weapons he may have ordered or attempted to order, the search history of JOHN DOE and other individuals at the UNIVERSITY whom SEGUI may have threatened or planned to harm, communications between SEGUI and JOHN DOE, threatening communications from SEGUI to other members of the UNIVERSITY, records related to SEGUI's purchase of bus tickets to travel to Michigan, records pertaining to JOHN DOE or JOHN DOE's schedule, SEGUI's other planning efforts for carrying out his threats against DOE and the content of any additional threatening emails SEGUI may have sent.

**COMPUTERS, ELECTRONIC STORAGE AND FORENSIC ANALYSIS**

17. As described above and in Attachment B, this application seeks permission to search for records that might be found on the DEVICE located at the Parents' Apartment. Records in this case will be data stored on a computer's hard drive. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

18. *Probable cause.* I submit that there is probable cause to believe the records described in Attachment B will be stored on the DEVICE, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the



Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because

special software is typically required for that task. However, it is technically possible to delete this information.

- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

19. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on the DEVICE because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment



of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

- b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer

or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the

offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

- c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.



- e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

20. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

- a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for

forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

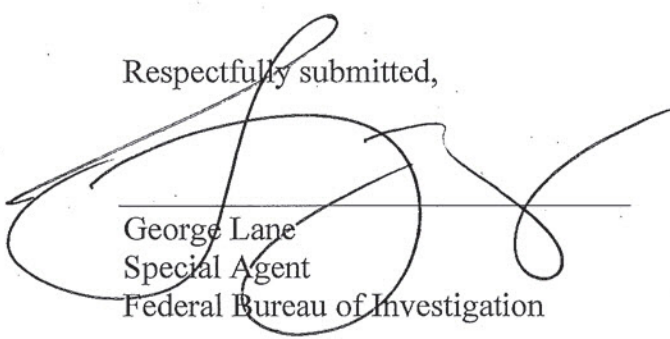
- b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.
  - c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.
21. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging or otherwise

copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

**CONCLUSION**

22. I submit that this affidavit supports probable cause for a warrant to search the DEVICE described in Attachment A and seize the items described in Attachment B.

Respectfully submitted,



George Lane  
Special Agent  
Federal Bureau of Investigation

Subscribed and sworn to before me  
on March 12, 2019

THE HONORABLE RAMON E. REYES, JR.  
UNITED STATES MAGISTRATE JUDGE  
EASTERN DISTRICT OF NEW YORK



**ATTACHMENT A**

*Property to be searched*

The property to be searched is a black Lenovo ThinkPad with the model number E67 and machine type 2522, and the serial number R8-B474X (the “DEVICE”). A picture of the DEVICE is below.



**ATTACHMENT B**

**Property to be Seized**

1. All records relating to violations of Title 18, United States Code, Sections 2261(A)(1), 2261(A)(2) and 875 (collectively, the “Subject Offenses”), involving FRANK SEGUI after January 1, 2018, including:
  - a. Evidence concerning the procurement, receipt, storage or shipping of an axe in or about 2019, and any communications about the aforementioned subjects;
  - b. Emails and other communications with members of the UNIVERSITY, including John Doe;
  - c. Internet search history, billing and payment records, and any other records related to the purchase of an axe in or about 2019;
  - d. Internet search history, billing and payment records, and any other records related to the purchase of bus tickets to Michigan in or about February 2019;
  - e. Any and all documents and records pertaining to John Doe or John Doe’s schedule;
  - f. Diaries, notebooks, notes and other records reflecting personal contact and other activities with John Doe; and
2. All documents used as a means to commit the Subject Offenses;
3. Evidence of who used, owned, or controlled the DEVICE at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence;
4. Evidence of software that would allow others to control the DEVICE, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
5. Evidence of the lack of such malicious software;
6. Evidence indicating how and when the DEVICE was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

7. Evidence indicating the DEVICE user's state of mind as it relates to the crime under investigation;
8. Evidence of the attachment to the DEVICE of other storage devices or similar containers for electronic evidence;
9. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the DEVICE;
10. Evidence of the times the DEVICE was used;
11. Passwords, encryption keys, and other access devices that may be necessary to access the DEVICE;
12. Documentation and manuals that may be necessary to access the DEVICE or to conduct a forensic examination of the DEVICE;
13. Records of or information about Internet Protocol addresses used by the DEVICE;
14. Records of or information about the DEVICE's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
15. Contextual information necessary to understand the evidence described in this attachment; and
16. Routers, modems, and network equipment used to connect computers to the Internet.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic,



or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term “storage medium” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.